ELECTRONIC CASH CONTROLLED BY NON-HOMOMORPHIC SIGNATURES

ABSTRACT

A method and system for establishing and managing digital cash. This method is to emit and circulate secure electronic cash that allows to use non-homomorphic signature schemes, and avoids having to use blind signature techniques. With one specific embodiment, the method provides anonymous digital cash, and comprises the steps of providing an entity with a secure coprocessor, a user establishing a secure channel to a program running on said coprocessor, and the user sending a coin to be digitally signed to the coprocessor.